THE DIGITAL CONTENT ENCRYPTION APPARATUS AND METHOD THEREOF

BACKGROUND OF THE DESCRIPTION

1. Field of the invention

The present invention is related to the encryption apparatus and the method thereof, and more particularly to the encryption apparatus and the method thereof which encrypts and transmits the digital content from the digital content transmission system by using the key information, the user key and the temporary validation key, to decrypt and replay the encrypted digital content in the user terminal by using the key information and the user authorization information.

2. Description of the Prior Art

Recently, people live in the midst of flood of information provided by various kinds of media such as broadcasting and press. This atmosphere created the information providers interested in providing the integrated information covering all the media and also there appeared users who want to selectively get a specific digital content out of the digital contents provided by the information provider (IP).

Accordingly, there appeared a digital content transmission system comprising the information providers who converts various information into the digital contents and stores this digital contents, and the users who are provided with this digital content from the IP by the network.

The digital content transmission system has provided an application program with easy downloadability of the digital contents. The user can get all the information he wants by accessing the digital content system through the network and using this application program.

The above mentioned digital contents are provided to the user for pay or for free. In case of the paid digital contents, the server with the digital content transmission system sets service fee. The service server charges the user according to the quantity of

used information when the charged digital content is downloaded to the user.

However, in case the user is connected to the server which provides the digital content commercially by the network, most of the users get an illegally copied and distributed digital content and this is very damaging to the server with a digital content transmission system.

SUMMARY OF THE INVENTION

The present invention is aimed at providing the digital content encryption apparatus and method thereof, which encrypts and transmitts the digital content from the digital content transmission system by using the key informtion, the user key and the temporary validation key, to decrypt and replay the encryted digital content in the user terminal by using the key information and the user authorization information.

Also, another purpose of this invention is to provide the digital content encryption communication protocol formed into a predetermined format for encryption of the digital content, according to which protocol the terminal unit decrypts the encrypted digital content.

To achieve the above-mentioned objects, a digital content encryption apparatus of the digital content transmission system comprises a terminal unit downloading and storing encryption key information requested by a user after the user registers member information including user's identity characters, said terminal unit decrypting a downloaded digital content using a decryption algorithm and the encryption key information to replay the digital content, and a service server generating the encryption key information corresponding to the identity characters from the terminal unit, said service server transmitting the encryption key information to the terminal unit, said service server encrypting the digital content using the encryption key information, said terminal unit downloading the encrypted digital content from the service server.

A digital content encryption apparatus of the digital content transmission system according to the present invention comprises a protocol format generator for generating a copyright protection protocol format, said protocol format generator generating a user key for encrypting a temporary validation key using a key generation algorithm

and key information, said key information being generated according to identity characters of a user, said protocol format generator generating a header using the user key to generate a temporary validation key, said generator adding encrypted digital content encrypted by the temporary validation key to the header to generate the copyright protection protocol format, and means for decrypting the copyright protection protocol format, said means receiving the generated copyright protection protocol format generated from the protocol format generator and then decrypting it using key information and a decryption algorithm to decrypt a user key and a temporary validation key, said means decrypting the encrypted digital content using the temporary validation key.

A protocol format for copyright protection of digital content according to the present invention includes a header field and an encrypted digital content field.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic block diagram showing one embodiment of the digital content encryption/decryption apparatus according to the present invention;

Fig. 2 is a drawing illustrating one embodiment of the terminal unit of Fig. 1;

Fig. 3 is a schematic block diagram showing another embodiment of the digital content encryption apparatus of Fig. 1;

Fig. 4 is a drawing illustrating one embodiment of the terminal unit of Fig. 3;

Fig. 5 is a block diagram showing the detailed functioinal sutructure of the digital content encryption apparatus of Fig. 1;

Fig. 6 is a block diagram showing the detailed functioinal sutructure of the digital content encryption apparatus of Fig. 3;

Fig. 7 is a flow chart illustrating the operation of the service server applied to Fig. 3;

Fig. 8 is a flow chart illustrating the operation of the host server applied to Fig. 3;

Fig. 9 is a schematic block diagram showing the functional structure of the digital content encryption apparatus according to the present invention;

Fig. 10 is an illustration of the protocol format applied to the present inven-

tion;

Fig. 11 shows another embodiment of the protocol format of Fig. 10;

Fig. 12 illustrates the header field applied to Fig. 10 and Fig. 11;

Fig. 13 shows another embodiment of the header field of Fig. 12;

Fig. 14 illustrates the unencrypted header field applied to Fig. 12 and Fig. 13;

Fig. 15 shows another embodiment of the unencrypted header field of Fig. 14;

Fig. 16 illustrates the detailed user authorization information applied to Fig. 14 and Fig. 15;

Fig. 17 is a drawing illustrating the detailed header field applied to Fig. 12 and Fig. 13;

Fig. 18 is a flow chart illustrating the method of generating the protocol applied to the present invention;

Fig. 19 is a flow chart illustrating the method of generating the header applied to Fig. 18;

Fig. 20 is a flow chart illustrating the method of generating the user authorization information applied to Fig. 19;

Fig. 21 is a flow chart illustrating the method of decrypting and replaying the encrypted digital contents according to the present invention;

Fig. 22 illustrates schematically the structure of the replaying device applied to Fig. 1 and Fig. 3; and

Fig. 23 is a flow chart illustrating the method of decrypting the encrypted digital contents.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention will now be described in detail referring to the accompanying drawings.

The present invention uses three keys in order to encrypt and decrypt the digital contents, which keys are explained below in detail.

First, key information is generated in the host server in response to the request of the service server when the user provided with the digital contents is unregistered.

The generated key information is stored in the user's terminal unit after transmitted through the service server.

In case of the digital content transmission system which combines the host server and the service server, the key information can be also generated in the service server.

The key information is used as means for getting a temporary validation key in the decryption process as well as in the encrytion process. Also, it is used as means for ascertaining whether the user is authrized to download and replay the encrypted digital contents in the user's terminal unit.

The key information is preferably generated by using random numbers and makes one-to-one correspondence with the user. Once generated, it is stored in the database of the host server with the user's characteritic charaters. The size of the key information is preferred to be 128 bytes.

Second, a user key is used for encrypting and decrypting the temporary validation key in the user authorization information of the header. It is generated by applying the forementioned key information to the key generation algorithm and used for generating and confirming the user's authorization information.

The user authorization information indicates a hash value of the user key generated by using the key information. When a hash value of the user key generated from the key information of the user proves the same as a hash value in the use authority of the header, the user is considered authrized to replay the encrypted digital contents.

To sum up, the user key is generated by using the key information and used for encryting the temporary validation key included into the user authorization information of the headerm. It is also used by the user to decrypt the encrypted temporary validation key, which is used to decrypt the encrypted digital contents.

Here the hash has features of always getting the same output from the same input and never inferring the input from the output, which features the present invention puts its basis on.

Third, a temporary validation key is used for encrypting a part of the digital contents and the header. It is preferably generated by using random numbers and its size

is determined to be a multiple of 8 bytes. It is preferred to be 8 byte in the present invention.

The temporary validation key has a feature that two temporary validation keys with the same content are not generated. For instance, the temporary validation key can be generated according to the time when the user accesses the service server. Accordingly, even the same user has the different temporary validation keys according to his access time. The temporary validation key exists valid only while the user accesses the system, that is, temporarily.

The present invention uses a plurality of algorithms, which include key generation algorithm, hash algorithm, and digital content encryption/decryption algorithm.

The key generation algorithm generates the user key by using the key information from the host server. In case of host server separate from service server, it is included in the service server.

The digital content encryption algorithm is also inclued in the service server and generates the header information to encrypt the digital contens.

The hash algorithm is used when the use autorization information is generated by using the user key in the service server or when it is ascertained whether the user is authorized.

To describe the digital content briefly, the digital content means a sort of data, e. g., music data, converted into digital signal which is stored in the form of a single file. The user can select the digital content stored in the form of file through the network access and read or listen to it by using a PC with an application program for communication or a replaying device connected to the PC.

The digital content includes all the information convertible into the digital data by the provider to be stored in the form of file, such as a magazine, a book, a dictionary and a drawing as well as a song.

Fig. 1 is a schematic block diagram showing one embodiment of the digital content encryption/decryption apparatus according to the present invention.

The terminal unit 10 transmits the user's identity characters and receives and stores the key information, which is generated in the service server 12 and corresponds

to the identity characters. It is also received from the service server 12 the protocol with the encrypted digital contents requested by the user, and decrypts and replays it by using the stored key information and the decryption algorithm.

The service server 12 generates the header with the user authorization information including the temporary validation key encrypted by the user key, and adds the encryted digital content to the header to generate the protocol for copyright protection. The protocol for copyright protection is transmitted to the user's terminal unit through network.

The terminal unit 10 is a personal computer (PC) 11a connected to the Internet. Also, the terminal unit 10 is applicable to any kind of apparatus equipped with a communication program for connection to the Internet. The good examples of the foregoing terminal unit 10 would be digital TV, cellular phone and web videophone. For example, the terminal unit with a network access program can be connected to a public switched telephone network or a wireless network.

Fig. 2 is a drawing illustrating one embodiment of the terminal unit of Fig. 1, where a terminal unit 10 is composed of a PC 11a equipped with the conventional communication device and a replaying device 11b. The PC 11a and replaying device 11b are provided with a plurality of decryption algorithm.

The PC 11a receives the key information from the service server 12 and stores it. Also, the PC 11a receives the protocol including the encrypted digital contents and records a storage medium such as HDD. It also generates the user key by using the stored key information, decrypts the temporary validation key by using the generated user key, and decrypts the encrypted digital contents by using the encrypted temporary validation key. As a result, the encrypted digital contents are replayed through a display or an audio device equipped by the PC 11a even without an additional replaying device 11b.

The replaying device 11b receives the key information and the encrypted digital contents from the PC 11a and decrypts the encrypted digital contents by using the stored decryption algorithm.

The replaying device 11b is either portable or stationary type according to the

type of the storage media.

The service server 12 generates key information corresponding to the identity characters transmitted from the terminal unit 10, stores the key information with the identity characters, and transmits it to the terminal unit in case the user requests the key information. The service server 12 generates the temporary validation key in response to the user's request, generates the user key by the key inforamtion, and generates the user authorization information from the temporary validation key encrypted by using the user key and a hash value of the user key. It also adds the digital contents encrypted by the encryption algorithm to the header with the user authorization information to form the copyright protection protocol and then transmits it to the terminal unit 10.

The service sanction agent server 14 receives the signal related to the digital content fees for downloading the digital content from the service server 12 and charges the user by accumulating the digital content fees of the registered user.

The identity characters are preferred to be the user's resident registration number, but any characters would be available only if they can identify the user like driver's license number.

Fig. 3 is a schematic block diagram showing another embodiment of the digital content encryption apparatus of Fig. 1. The explanation related to the terminal unit 20, the replaying device 21b and the service sanction agent server 24 will be omitted since they were described in the Fig. 1.

The service server 22 transmits to the host server 23 the request signal for the key information corresponding to the identity characters transmitted from the terminal unit 20. According to the request signal, the host server 23 transmits the key information to the service server, which key is then transmitted to the terminal unit 20.

Also, the service server 22 transmits the key information to the terminal unit 20 in response to the user's request. The service server 22 generates the temporary validation key in response to the user's request, generates the user key by the key inforamtion, and generates the user authorization information from the temporary validation key encrypted by using the user key and a hash value of the user key. It also adds the digital contents encrypted by the encryption algorithm to the header with the user authorization

information to form the copyright protection protocol and then transmits it to the terminal unit 20.

The host server 23 generates the key information corresponding to the identity characters transmitted from the service server 22 and stores it with the identity characters, then transmitting it to the service server 22 in response to the request signal of the service server 22.

In Fig. 1 and Fig. 3, the service server 12 and 22 can have a digital content list, with which the digital content provider can inform the user of the digital content he retains and the user is easy to select the digital content he wants. For example, the digital content list would be the title of the song, the name of singer etc. if the digital content is music data.

Fig. 5 is a block diagram showing the detailed functioinal structure of the digital content encryption apparatus of Fig. 1, where the functional structure of and the interrelation between the service server and the terminal unit are shown.

As shown in Fig. 5, the terminal unit 200 comprises an interface 201, a use authority identifier 202, a temporary validation key decryptor 203, and a digital content decryptor 204.

The interface 201 receives the key information generated corresponding to the user's identity characters. The use authority identifier 202 generates the user key after reading the header of the protocol received from the service server 210 and then identifies whether the user is authorized by analyzing the user authorization information with the generated user key. The temporary validation key decryptor 203 decrypts the temporary validation key using the user key. The digital content decryptor 204 decrypts the encrypted digital content using the temporary validation key decrypted by the temporary validation key decryptor 203.

The service server 210 comprises an interface 218, key information generator 212, a user key generator 213, a temporary validation key generator 214, a user authorization information generator 215, a header generator 216, and a protocol format generator 217.

The interface 218 receives the identity characters input from the terminal unit

200. The key information generator 212 determines whether the identity characters input from the interface 218 exist in the database 211, and then generates the key information. The user key generator 213 generates the user key by applying the key information to the key generation algorithm. The temporary validation key generator 214 generates the temporary validation key when the user accesses the service server 210 through the interface 218 and requests the digital contents. The user authorization information generator 215 generates the use authority key information by encrypting the temporary validation key using the user key generated by the user key generator 213 and then using the user key and the encrypted temporary validation key. The header generator 216 generates the header using the user authorization information and additional information necessary for encryption. The protocol format generator 217 generates the copyright protection protocol by adding the encrypted digital content to the header generated by the header generator 216.

The operation of the digital content encryption/decryption apparatus of Fig. 5 would be described below briefly.

When the user inputs the identity characters in order to get the digital contents from the service server 210, the service server 210 receives them through the interface 218 and outputs them to the key information generator 212.

Then, the key information generator 212 determines whether the identical ones with the input identity characters exist among the identity characters registered to the database 211. According to the result of determination, the key information generator 212 generates the new key information corresponding to the identity characters to transmit the key information to the user key generator 213 or transmits the registered key information to the user key generator 213.

The user key generator 213 generates the user key by applying the key information to the key generation algorithm and then outputs the user key to the key information generator 215.

The temporary validation key generator 214 generates the temporary validation key in response to the user access signal input through the interface 218 and inputs it to the key information generator 215.

The user authorization information generator 215 calculates the hash value by applying the user key to the hash algorithm, then encrypts the temporary validation key using the user key, and generates the user authorization information from a set of the hash value and the encrypted temporary validation key. The generated user authorization information is input to the header generator 216.

The header generator 216 adds the user authorization information to the header and then outputs it to the protocol format generator 217.

The protocol format generator 217 forms the protocol format by adding the encrypted digital content to the header and then transmits it to the terminal unit 200.

Fig. 6 is a block diagram showing the detailed functioinal structure of the digital content encryption apparatus of Fig. 3, where the functional structure of and the interrelation between the service server, the host server and the terminal unit are shown.

In Fig. 6, the key information generator 111 and the database 122 belong to the host server 120. Also, the user key generator 111, the interface 115, the temporary validation key generator 112, the user authorization information generator 113, the header generator 114, and the protocol format generator 114 belong to the service server 110. Description about the operation of each unit will be omitted, as the operation of each unit is the same as in case of Fig. 5.

In the above, the illustration of the present invention was made mostly referring to the PC user. However, it can be applicable to any kind of device equipped with a communication program and a decrytion algorithm.

Fig. 7 is a flow chart illustrating the operation of the service server applied to Fig. 3, which is related to the case the user unregistered to the service server intends to be provided with the digital contents.

The service server 22 can be accessed from the terminal unit 20 by the network access program. When the user inputs his identity characters, the service server identifies whether he is registered by comparing the input identity characters with the registered ones. If the user is registered, the key information is not generated additionally. If the input identity characters are determined not to exist in the service server 22, however, the service server 22 recognizes the user as a new member and proceeds into the mem-

bership registration.

If the user who wants to get the digital content makes the membership registration, the service server 22 receives the key information from the host server 23 and then transmits it to the terminal unit 20 in response to the user's request (S510).

The above mentioned key information generated in response to the identity characters is maintained valid unless the user applies the cancellation of his membership.

After the step of S510, the service server 22 determines whether the request signal for downloading the digital contents is received from the terminal unit 20 (S520). If the request signal for downloading is determined to be received, the service server 22 generates the user key using the key information, encrypts the temporary validation key using the user key, and then generates the header using the user key and the encrypted temporary validation key. It also generates the copyright protection protocol by adding the encrypted digital contents to the header and transmits the protocol to the user (S530).

After transmitting the digital content to the user, the service server 22 transmits the service fee information to the service sanction agent server 24 in order to add it to the stored service fee information. The service sanction agent server 24 charges the user for the digital content he used by using the service fee information.

Fig. 8 is a flow chart illustrating the operation of the host server applied to Fig. 3.

As shown in Fig. 8, the host server 23 determines whether the identity characters are received (S610).

When it is determined that the identity characters are received, the received characters are compared with the identity characters stored in the database to determine whether the identical identity characters exist (S620).

After the above step of S620, the key information stored with the identity characters are transmitted to the service server 22 when the identical identity characters are found (S630), while the key information is generated (S640) and then the generated key information is stored with the identity characters (S650) when the identical identity

characters are not found.

The step of S510 carried out by the service server 22 and the steps of S610 to S650 carried out by the host server 23 are carried out in case a service server 22 and a host server 23 are provided separately as in Fig. 2. When only a single service sever 11 is provided, however, the service server 11 integrally carries out the above mentioned steps to generate the key information corresponding to the user's identity characters and then transmit the generated key information to the user, which steps are not specifically described since the processes can be easily inferred from Fig. 7 & 8.

The terminal units 10 and 20 are provided with the key information and the digital contents, decrypts them through the stored decryption algorithm and at the same time outputs them to the external or internal audio output device to render them audible to the user.

Therefore, when illegal copying of the digital content from the terminal unit 10 and 20 to another terminal unit occurs, the absence of the key information within the other terminal unit will disable the encrypted digital content from being replayed and heard.

In case the registered user wants to provide another person with the digital contents, the identication charaters of the another person is stored with the identification charaters of the registered user. In thi case, the encrypted digital contents are decrypted and replayed with the former identification charaters as well as with the latter ones.

The fee for the provided digital contents would be paid by the user registered to the service server 22.

In the functional aspect, the digital content encryption/decryption apparatus according to the present invention can be divided broadly into the device encrypting the digital content and the device decrypting the encrypted digital content.

Fig. 9 is a schematic block diagram showing the functional structure of the digital content encryption apparatus according to the present invention.

The digital content encryption apparatus of the present invention consists of a protocol format generator 30 and a protocol format decoder 31.

The protocol format generator 30 generates the copyright protection protocol

format consisting of the encrypted digital contents and the header including the information necessary for encrypting and decrypting the digital contents. The protocol format decoder 31 decrypts and replays the encrypted digital contents from the copyright protection protocol format input from the protocol format generator 31 according to the header information of the protocol format.

More particularly, the protocol format generator 30 generates the user key by using the key information generated corresponding to the user's identity characters and the key generation algorithm. Then, it generates the header to which the user authorization information with the encrypted temporary validationkey is added using the user key and a hash value of the user key. It also generates the copyright protection protocol format by adding the encrypted digital content encrypted by the temporary validation key to the header.

The protocol format decoder 31 receives the copyright protection protocol format generated by the protocol format generator 30 to generate the user key using the key information, and decrypts the encrypted digital content using the temporary validation key after decrypting the temporary validation key using the user key in case the user is identified to be authorized. It is idenfied through the user authorization information which is achieved using the user key whether the user is authorized.

Operation of the protocol format processing system will be described in detail referring to the appended Fig. 10 and Fig. 16.

When the user selects the digital content he wants to be provided with, the digital content encryption apparatus of the present invention forms the digital content into the protocol format described below and then transmits it to the user.

Fig. 10 is an illustration of the protocol format applied to the present invention. The protocol for protecting the copyright of digital information comprises a header, which includes information for encrypting the digital contents and information for explaining the digital contens, and an encrypted digital content field.

The structure of the header will be described in detail referring to Fig. 5. The encrypted digital contents are encrypted partly by the user key and the temporary validation key so as not to replay in case of the absence of the key information.

Fig. 11, which illustrates another embodiment of the protocol format of Fig. 10, shows the copyright protection protocol including additional fields optionally added.

A field for indicating the size of an encrypted digital content is inserted between the header and the encrypted digital content field, which size is preferred to be the same as that of the unencrypted digital content field.

Also, the additional information field can be added to the rear end of the encrypted digital content field in order to define the encrypted digital contents for user's easy understanding.

In case the digital content is song data, for example, the additional information would be various data such as the singer, title of songs, playing time, title of albumn, the maker of albumn, publishing date, moving pictures of music video.

The additional information field is formed in a format that the header and the data are arranged in turnn, so it can be expanded regardless of the number of additional information.

Fig. 12 illustrates the header field of Fig. 10 and Fig. 11 more particularly, which comprises a copyright support information field, an unencrypted header field and an encrypted header field.

The copyright support information field includes the copyright support code showing whether the digital content provided by the digital content provider supports the copyright.

If the copyright support code exists in the copyright support information field, the digital contents provided to the user is recognized to be encrypted, and then decrypted to replay. Otherwise the digital content is recognized to be unencrypted and the decryption process is terminated in order for the digital contents to be replayed without decryption.

Fig. 13 shows another embodiment of the header field of Fig. 12. Fig. 11, which field includes optionally added additional fields.

An offset field and a field for indicating the size of the unencrypted header are inserted between the copyright support information field and the unencrypted header field. The offset field provides information on the position of the additional information

field, which enables the additional information field to be accessed without analysis of the header. Also, a field for indicating the size of the encrypted header is provided prior to the encrypted header field.

Fig. 14 illustrates the unencrypted header field applied to Fig. 12 and Fig. 13.

The unencrypted header field comprises a copyright library version field, a digital conversion format field for indicating the type of the digital conversion format, a key generation algorithm field for indicating the information on the key generation algorithm, a digital content encryption algorithm field for indicating the information on the digital content encryption algorithm, a field for indicating the user authorization information at PC, and a field for indicating the user authorization information at the replaying device.

The digital conversion format field shows in what conversion method the digital content is converted into the digital signal. Typical examples of the conversion method are MP3 and AAC.

The encryption algorithm field includes hash algorithm code, key encryption algorithm code, the size of initial vector (IV), the information on initial vector used for encrypting the digital contents.

The field for indicating the user authorization information at PC and the field for indicating the user authorization information at the replaying device are the most important in the header, which serve to identify the user's authority to use the digital cotents and increase in proportion to the number of peaple who share the encrypted digital contents.

Fig. 15, illustrating another embodiment of the unencrypted header field of Fig. 14, shows the unencrypted header field including optionally added additional fields.

A field for indicating the code of digital content provider is inserted between the digital content conversion format field and the key generation algorithm field. To the rear end of the digital content encryption algorithm field can be added a field of the number of users sharing the PC, a field of the number of users sharing the replaying device.

Fig. 16 illustrates the detailed structure of the user authorization information

fields applied to Fig. 14 and Fig. 15.

The user authorization information fields at PC and at the replaying device comprise a field for indicating the size of hash value generated by hash algorithm, a field for indicating a hash value of the user key, a field for indicating the size of resultant value of the encrypted temporary validation key generated by key encryption algorithm, and a field for indicating the resultant value of the encrypted temporary validation key.

Fig. 17 is a drawing illustrating the detailed header applied to Fig. 12 and Fig. 13.

The encrypted header field comprises a field for indicating the basic process unit of the digital contents, a field for indicating the number of the encrypted bytes, a field for indicating the encrypted frame unit, and a hash value field for determining the state of entire header.

The basic process unit of the digital contents and the number of the encrypted bytes can be assigned by the information provider. However, they are possibly set the basic values by a basic algorithm referring to the processing speed of a terminal unit and a memory.

A hash value in the hash value field indicates a hash value of both the copyright support information field and the unencrypted header field, i.e., a hash value of the fields prior to the encrypted header field within the header field.

Fig. 18 is a flow chart illustrating the method of generating the protocol applied to the present invention.

When the digital content request signal is input from the user, the temporary validation key is generated (S110). Then, it is determined whether the header generation algorithm defined by the digital content provider exists when the temporary validation key is generated (S120).

In case of existence of the header generation algorithm at the determination step of S120, the header is generated by the header generation algorithm defined by the digital content provider (S130). In case of non-existence of the header generation algorithm, the header is generated in a basic value (S190).

After the header is generated at the step of S130 or S190, the digital content is encrypted (S140) and then added to the header generated at the step of S130 or S190 (S150).

In case that the additional information is provided, it is determined whether the additional information to the digital contents combined with the header exists (S160). If the additional information is determined to exist at the step of S160, the additional information field is generated (S170) and added to the rear end of the encrypted digital content (S180) to form the copyright protection protocol. The copyright protection protocol is then transmitted to the user who want the digital contents.

The additional information to the digital contents is added optionally by the provider when the provider would like to make an additional explanation about the digital contents to the user. The additional information processing step of S220 can be added selectively by the service provider.

Fig. 19 is a flow chart illustrating the method of generating the header applied to Fig. 18.

The copyright support information field, describing whether the digital contents provided is under the protection of copyright, and a field for indicating the size of unencrypted header are generated and added to the header (S210). The unencrypted header field is also generated and added to the header (S220), which field includes the version information, a type of music, the code of service provider supporting the copyright, hash algorithm, key generation algorithm, and digital content encryption algorithm.

If the additional information field of the digital contents exists, information on the starting point of the additional information field can be also added to the header.

At step of S220 that a part of the header part is constructed, the user authorization information is generated using the key information the user has and the generated user authorization information is added to the header (S240). Following the step of S240, the encrypted header information is generated (S250).

The header information includes information necessary for encryption of the digital content such as size of the encrypted block, encryption period and encrypted

frame unit, etc. The header information is also generated to include the hash value by applying the whole header to the hash algorithm, with which value the change of header information can be determined.

The header information generated at the step of S250 is encrypted (S260) and then the information on the encrypted header and the size of the encrypted header is added to the header (S270), so that generated is the header added to the front end of the encrypted digital content transmitted to the user.

In case the encryption algorithm provided by the digital content provider exists (S260), the header information is encrypted by the encryption algorithm and the temporary validation key. Otherwise the header information is encrypted by the basic algorithm and the temporary validation key.

Fig. 20 is a flow chart illustrating the method of generating the user authorization information applied to Fig. 19, which describe in more detail the method of generating the encryption key information at the step of S230 of Fig. 19.

It is determined whether the key information or the temporary validation key exists (S310). The user key is generated by applying the key information to the key generation algorithm when it is determined that the key information and the temporary validation key exist at the step of S310 (S320).

A hash value is calculated by applying the user key generated at the step of S320 (S330) to hash algorithm, and then the temporary validation key is encrypted using the key encryption algorithm and the generated user key (S340). At the determination step of S310, the process is terminated with output of message of error when the key information or the temporary validation key is determined not to exist.

Fig. 21 is a flow chart illustrating the method of decrypting and replaying the encrypted digital contents according to the present invention.

First, it is determined whether the key information or the digital contents received from the digital content provider exists (S410). The header of the digital contents is read when either the digital content or the key information is determined to exist (S415), and the process is recognized to be an error and terminated when the digital contents and the key information do not exist (S480).

It is determined whether the header read at the step of S415 includes the copyright support code, that is to say, whether the digital content supports the copyright (S420).

If the copyright support code is determined to exist, the digital contents are recognized to be protected by copyright and the read unencrypted header information is stored at a memory as a predetermined variable (S425).

If the copyright support code is determined not to exist, that is, the digital contents are not protected by copyright, the digital contents is recognized to be an error in the decryption process. Then the decryption process is no longer carried out and the received digital contents are decoded and output, not passing through decryption process.

When the digital content is determined to be supported by copyright, the user key is generated using the key information and then the hash value of the generated user key is calculated (S430).

It is determined whether the calculated hash value of the user key is identical with a hash value of the user key in the header (S435).

When the calculated hash value of the user key is determined to coincide with the hash value of the user key in the header, the user is recognized to be authorized and the temporary validation key is decrypted using the user key (S440). The encrypted header is decrypted using the decrypted temporary validation key (S445). The hash value of entire header, which is served as a reference value for determination the change of entire header, is calculated by applying the entire header to hash algorithm (S450).

At the determination step of S435, the message of "Not authorized" is output and the entire digital content decryption process is terminated when the calculated hash value of the user key is determined not to be identical with the hash value of the user key in the header.

The change of the header is determined according to hash value of the entire header (S455). In case the header is determined not to be changed, the encrypted digital contents are decrypted (S455).

It is determined whether additional information exists (S465). The digital contents are replayed if the additional information is not determined not to exist (S470).

The additional information is processed and then replayed when the additional information is determined to exist (S475).

When the header is determined to be changed at the step of S455, the user is recognized not to be authorized so that the decryption process is terminated for the user not to replay the digital contents (S490).

Fig. 22 illustrates schematically the structure of the replaying device applied to Fig. 1 and Fig. 3.

Memory 300 includes a driving algorithm for the entire system and a plurality of algorithms for decrypting the encrypted digital contents. Memory 300 stores in itself the received key information and digital content data in response to the writing signal and outputs the stored key information and digital content data in response to the reading signal. Memory 300 is preferred to be a flash memory.

Microcomputer 320 receives the key information and digital content data to store memory 300, decrypts the encrypted digital contents by the algorithm stored in memory 300 and then outputs them according to the key signal input from the user key input device 330. At the same time, it controls display 340 to display the present state of the apparatus.

Microcomputer 320 generates the user key through the user authorization information of the header using the key information stored in memory 300 according to the algorithm, which is also stored in memory 300, when the input digital contents are encrypted. Also, microcomputer 320 decrypts the temporary validation key included in the user authorization information of the header using the generated user key. The encrypted digital contents are decrypted using the decrypted temporary validation key to be output.

When the unencrypted digital contents are received, microcomputer 320 replays and outputs the digital contents without decrypting them.

Decoder 350 decodes the digital contents output from microcomputer 320 to output audio signal. Decoder 350 is preferred to be MPEG decoder.

Fig. 23 is a flow chart illustrating the method of decrypting the encrypted digital contents in case the encrypted digital contents are input from PC to the replaying de-

vice constructed as in Fig. 22 .

Microcomputer 320 determines whether the key information is input from PC (S510) and stores the input key information in memory 300 when the key information is determined to be input (S515).

After storing the key information in memory 300, microcomputer 320 determines whether the encrypted digital contents are input from PC (S520). When the encrypted digital contents are determined to be input at the step of S520, microcomputer 320 stores the digital contents in memory 300 and then reads the header from the digital contents according to the decryption algorithm stored in memory 300 after the transmission process is completed (S525). When the encrypted digital contents are determined not to be input, they are recognized as an error (S580) and the decryption process is terminated.

Next, microcomputer 320 determines whether the copyright support code exists in the header of the read digital contents (S530).

If the copyright support code is determined to exist, the digital contents are recognized to be protected by copyright and the read unencrypted header information is stored at memory 300 as a predetermined variable (S535).

When the digital contents is determined to be protected by copyright, microcomputer 320 generates the user key using the key information and the key generation algorithm. Microcomputer 320 calculates a hash value of the generated user key by hash algorithm stored in memory 300 (S540).

Next, microcomputer 320 determines whether the calculated hash value of the user key is identical with a hash value of the user key in the user authorization information of the header (S545).

When the calculated hash value of the user key is determined to coincide with the hash value of the user key in the header, the user is recognized to be authorized and the temporary validation key is decrypted using the user key (S550). The encrypted header is decrypted using the decrypted temporary validation key (S555).

At the determination step of S545, a message of "Not authorized" is output and the decryption process is terminated when the calculated hash value of the user key is

determined not to be identical with the hash value of the user key in the header.

It is determined according to hash value of the entire header whether the entire header is changed in order to determine whether the user is authorized to decrypts and replay the digital contents (S455). The hash value is calculated by applying the entire header to hash algorithm (S560).

The change of the entire header is determined according to whether the hash value of the entire header calculated at the step of S560 is identical with a hash value of the entire header stored in the header (S565).

In case the header is determined not to be changed, that is, the hash value of the entire header calculated at the step of S560 is identical with the hash value of the entire header stored in the header, the encrypted digital contents are decrypted (S570). The additional information is processed and then replayed in case the additional information does not exist (S575).

When the header is determined to be changed at the step of S565, that is, the calculated hash value of the entire header is not identical with the hash value of the entire header stored in the header, the user is recognized not to be authorized so that the decryption process is terminated for the user not to replay the digital contents (S585).

In the present invention, the supplied encrypt digital content cannot be replayed without the supply of the decoding algorithm and the key information. Therefore, when the digital content is illegally copied, it cannot be replayed, preventing illegal copy and unauthorized distribution. This will prevent significant loses for the provider of the digital content caused by illegal copying and unauthorized distribution while forcing the user to acquire the digital content via a legitimate route.

While this invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.